МЕТОДЫ РАСПРОСТРАНЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

MALWARE DISTRIBURION METHODS

A. Snegirev
I. Marshalova
A. Vershinin
P. Nesterov
A. Vikulova

Summary. The article is an overview of real malware distribution methods and possible threats. This article shows the current malware distribution methods and schemes. The article fully discloses the spam and phishing threat and attacks and the example of phishing emails in this article examines a malicious attachment and shows one of the methods of infecting your computer with a malicious file.The functionality of a malicious file is considered in detail and examples of other possible methods and ways of its transmission, as well as ways of infecting information technologies are given. It also presents real statistics of spam and phishing present in the Russian Internet space and the most popular malicious attachment. The above information is sufficient to understand the dangers for both home and corporate Internet users, and the recommendations provided to prevent infection of the computer and not to become a victim of fraudsters using the "World Wide Web". This article will be of interest to analysts and specialists in the field of information security, in particular, providing a mechanism designed to protect information and information technologies from the impact of the malware.

Keywords: spam, phishing, backdoor, ransomware, botnet, macros, attack.

Снегирев Артем Игоревич
ФГБОУ ВО «МИРЭА- Российский технологический университет»
svasdva@gmail.com
Маршалова Ирина Юрьевна
ФГБОУ ВО «МИРЭА- Российский технологический университет»
irkimus@mail.ru
Вершинин Александр Николаевич
Старший преподаватель, ФГБОУ ВО «МИРЭА- Российский технологический университет»
ve.sa.2009@mail.ru
Нестеров Павел Александрович
ФГБОУ ВО «МИРЭА- Российский технологический университет»
Pavel123357@gmail.com
Викулова Анастасия Сергеевна
ФГБОУ ВО «МИРЭА- Российский технологический университет»
Nastya_1_vikulova@mail.ru

Аннотация. Статья носит обзорный характер реальных методов распространения и возможных угроз вредоносного программного обеспечения. В данной статье показаны актуальные методы и схемы злоумышленников по распространению вредоносного программного обеспечения. Статья полностью раскрывает угрозу спама и фишинговых атак и на примере фишингового письма, в данной статье разбирается вредоносное вложение и показывается один из методов заражения компьютера вредоносным файлом. Подробно рассмотрен функционал вредоносного файла и приведены примеры других возможных методов и способов его передачи, а также пути заражения информационных технологий. Также представлена реальная статистика спама и фишинга присутствующего в Интернет пространстве российских провайдеров и наиболее популярных вредоносных вложений. Приведенные сведения, достаточны для понимая всей опасности в целом как для домашних, так и для корпоративных пользователей Интернета, а предоставленные рекомендации позволяют предотвратить заражение компьютера и не стать жертвой мошенников использующих «всемирную паутину». Данная статья будет интересна аналитикам и специалистам в области информационной безопасности, в частности обеспечения механизма, предназначенного защитить информацию и информационные технологии от воздействия вредоносного программного обеспечения.

Ключевые слова: спам, фишинг, бэкдор, шифровальщик, ботнет, макрос, атака.

В наше время частое заражение компьютеров вредоносными программами происходит из-за невнимательности или доверчивости пользователей компьютеров. Например, качественно подделанное электронное письмо может содержать файл с вредоносным кодом, **эксплуатирующим** различные уязвимости в программных продуктах для заражения компьютера. Спам и фишинг являются двумя самыми эффективными техниками, которыми пользуются злоумышленники для распространения вредоносного программного обеспечения или, чтобы выудить деньги у доверчивых получателей. По мере того как всё больше людей становят-

Рис. 1. Мошенническая схема "кибер-группировки" Carbanak. [7]

Рис. 2. Обнаружение вредоносного файла Carbanak. [7]

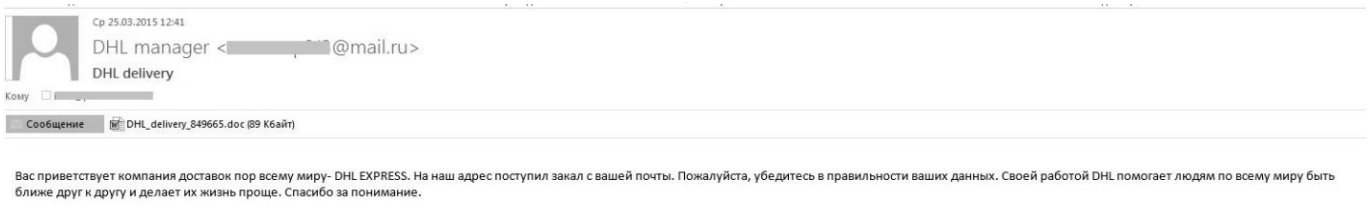

Рис. 3. Образец спам письма.

ся зависимыми от современных технологий, например, от Интернета, разного рода преступники объединяются в организации или "кибер-группы" и стараются осуществлять свои заранее обдуманные проекты, которые помогают им отнимать деньги от ничего не подозревающих добропорядочных пользователей. Например, нашумевшая в недавнем времени "кибер-группировка" Carbanak смогла заразить с помощью целевой рассылки электронных писем с прикрепленным вредоносным файлом в общей сложности около 100 банков из 30 стран (рис. 1, рис. 2). Приблизительный ущерб составляет 1 млрд. долларов США. [7]

Поскольку тема киберпреступлений очень распространена в наши дни, то в данной статье мы разберем, что это такое и какие могут быть последствия, если ваш компьютер подвергся данным атакам.

Термин «**Спам**» — это массовая рассылка информации рекламного или иного характера людям, не дававшим своего согласия на её получение. [1]

Термин «**Фишинг**» — вид мошенничества в Интернете, цель которого — собрать персональные данные пользователей для дальнейшего злонамеренного использования. К этому относятся кражи номеров кредитных карт, паролей, банковских счетов и любой другой конфиденциальной информации. [1]

Фишинг представляет собой входящие на почту псевдо-уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать или обновить личные данные. Причины могут быть различные. Это может быть поломка или утеря данных, в системе и прочее.

Различаются они методами атак.

Методы атак

Сложились вполне устойчивые методы действий пользователей, рассылающих спам:

- сбор и подтверждения e-mail- адресов получателей;
- подготовка компьютеров, через которые будет рассылаться спам;
- создание ПО для рассылки;
- поиск жертв;
- создание рекламных объявлений для конкретной рассылки;
- произведение рассылки.

Каждый отдельный шаг может выполняться независимо от другого.

А вот фишинговые атаки намного продуманнее, даже могут применяться методы социальной инженерии. В любом случае клиента сначала пытаются напугать: моделируют критическую ситуацию для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы или легкие деньги, например, выигрыш в лотерее или угроза блокировки счета в случае невыполнения требований, указанных в сообщении. [2]

Особенностью фишинговых писем является их высококачественная подделка. Адресат получает письмо с логотипами банка/ сайта/ провайдера, выглядящими в точности так же, как настоящие. Ничего не подозревающий пользователь переходит по ссылке «Перейти на сайт и ввести персональные данные», но на самом деле попадает не на официальный сайт, а на его аналог, выполненный с высокой точностью. [2]

Частые жертвы фишинга — это банки, платежные системы, аукционы. Мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться для рассылки вирусов или троянов (Backdoor) для создания зомби-сетей.

Хитростью фишеров являются ссылки, похожие на URL оригинальных сайтов, ведь даже опытный пользователь не всегда обратит внимание на то, что ссылка в браузере не является легитимной.

Разбор атаки

Многие пользователи Интернета пользуются онлайн сервисами, например, доставкой, платежными и банков-

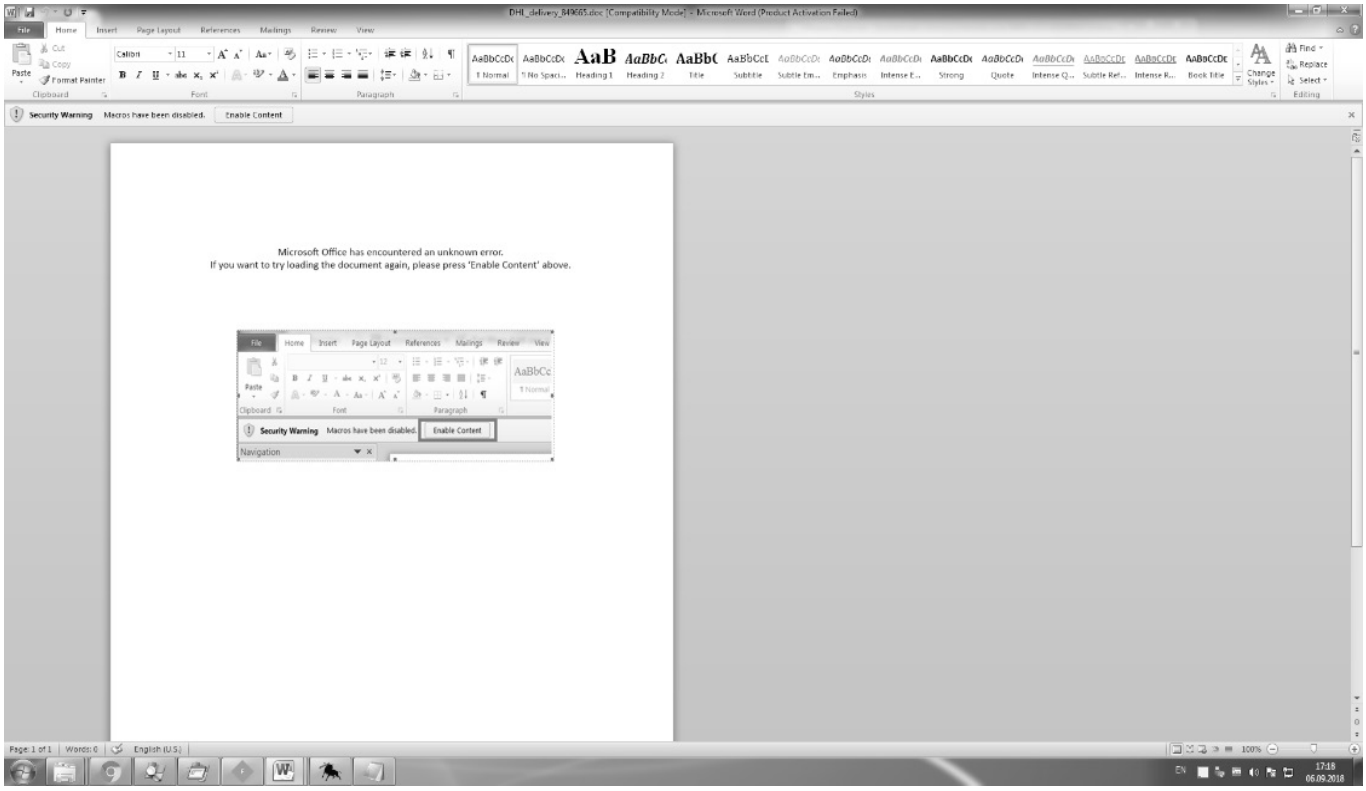

Рис. 4. Пример вредоносного файла.

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Sub AutoOpen()
Set x = GetObject("soap:wsdl=http://[redacted]/svchost.exe")
End Sub
```

Рис. 5. Код скрипта, встроенного в документ:

скими сервисами, и спам — атаки могут ввести их в заблуждение.

Схема, используемая злоумышленниками, проста — она не менялась на протяжении нескольких лет, но остается на редкость эффективной. [3]

Давайте рассмотрим актуальную на сегодняшний день спам — атаку. Вот так выглядит спам — письмо (рис. 3.) содержащее вложенный файл с расширением .doc и сообщение, заставляющее получателя проверить корректность своих данных для курьерской доставки.

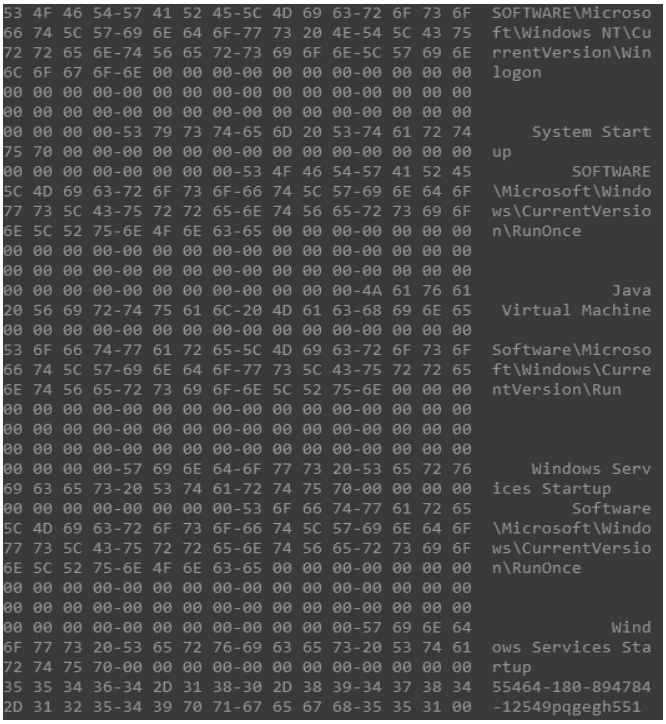

Рис. 6. Строки вредоносной активности файла svchost.exe

Рис. 7. Сетевые функции вредоносного программного обеспечения.

У пользователя файл с расширением.doc, скорее всего, не вызовет никаких подозрений, однако именно такие файлы (как.doc и.xls) очень часто используются злоумышленниками для распространения так называемых макровирусов — вредоносных скриптов, вставленных в файл как макрос. Многие не знают, что макрос, написанный на специальном языке VBA (Visual Basic for Applications), встроенный в документ Word или Excel, обладает функциями обычной программы и может использоваться в преступных целях. Чаще всего вредоносный код макроса для получения несанкционированного доступа в операционную систему. Например, скачать и запустить вредоносный файл.

Для обхода почтового антивирусного детектирования вложенные файлы могут быть защищены паролем, который прилагается в письме.

В открытом письме (рис. 4) нам сообщают, что возникла неизвестная ошибка, и для ее исправления нам нужно нажать на кнопку "Enable Content". Кнопка "Enable Content" активирует код вредоносного скрипта (Макроса) (рис. 5), содержащегося в документе.

После выполнения кода на компьютер пользователя загрузится и запустится файл с названием svchost.exe, функционал которого попадает под классификацию Лаборатории Касперского Backdoor.

Backdoor — предназначены для удаленного управления злоумышленником пораженным компьютером. По своим функциям Backdoor во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами— производителями программных продуктов.

Подобные вредоносные программы позволяют делать с компьютерами все, что в них заложит автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и так далее. [4]

Представители этого типа вредоносных программ очень часто используются для объединения компьютеров- жертв в так называемые ***ботнеты/зомби-сети***, что позволяет злоумышленникам централизованно управлять всей армией пораженных компьютеров для совершения злонамеренных действий, чаще всего

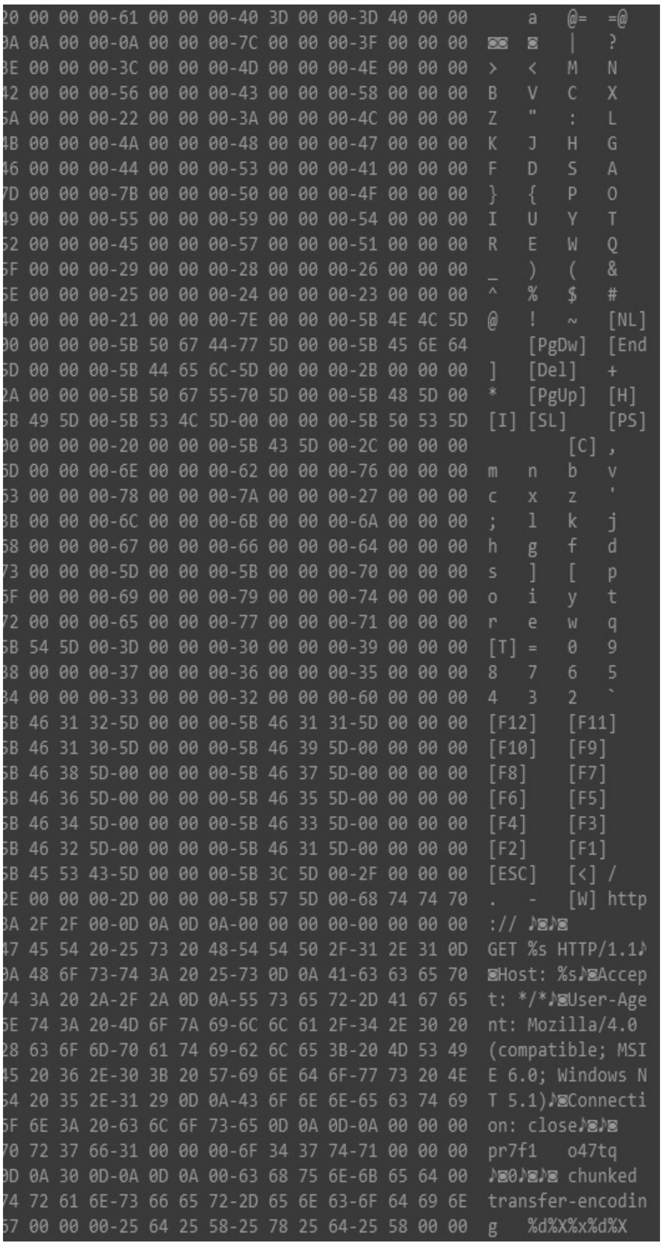

Рис. 8. Строки записи нажатия клавиш.

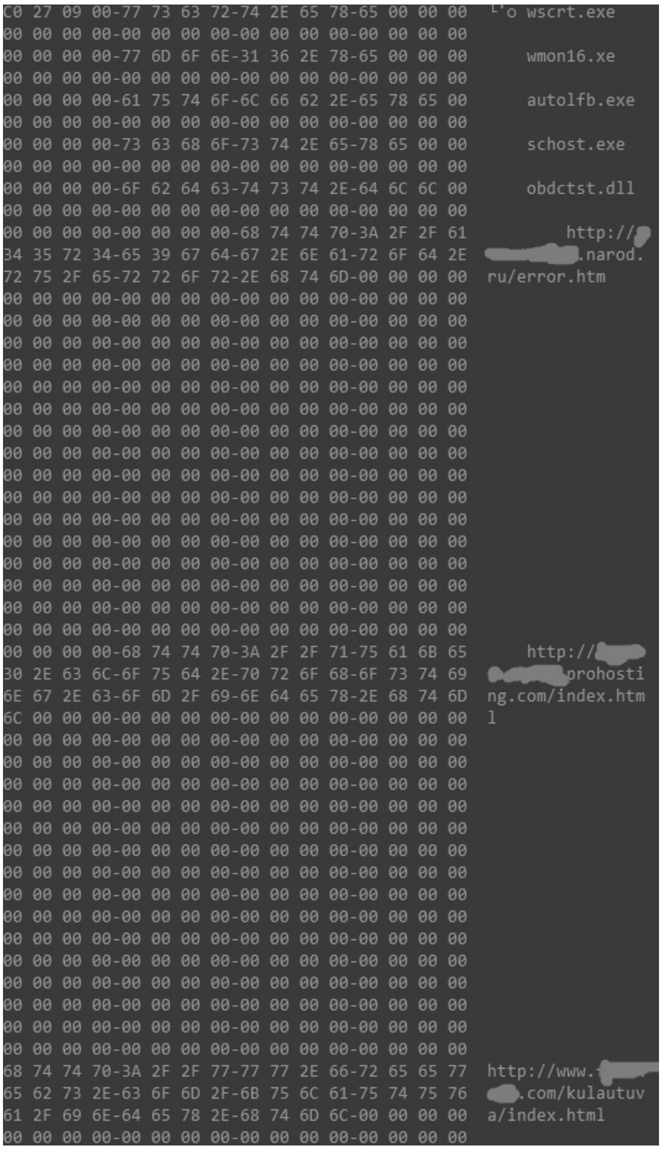

Рис. 9. Имена файлов и ссылки в теле вредоносного программного обеспечения.

с помощью сервера, который называют контроллером ботнета. Цель ботнета состоит в заражении как можно большего числа компьютеров и создании на их основе масштабной сети, которая может быть использована как для распространения другого вредоносного программного обеспечения или спама, так и для выполнения DDoS-атак (distributed denial-of-service — распределенный отказ в обслуживании). Если все зомби одновременно начнут атаковать определенный сайт, то он может стать недоступным. [5]

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

В нашем случае вредоносный файл сохраняет свою копию в папке%Temp% и добавляет себя в автозагрузку (рис. 6), чтобы перезагрузка компьютера не препятствовала его работе.

Затем подключается к удаленному командному серверу злоумышленника для получения дальнейших команд (рис. 7).

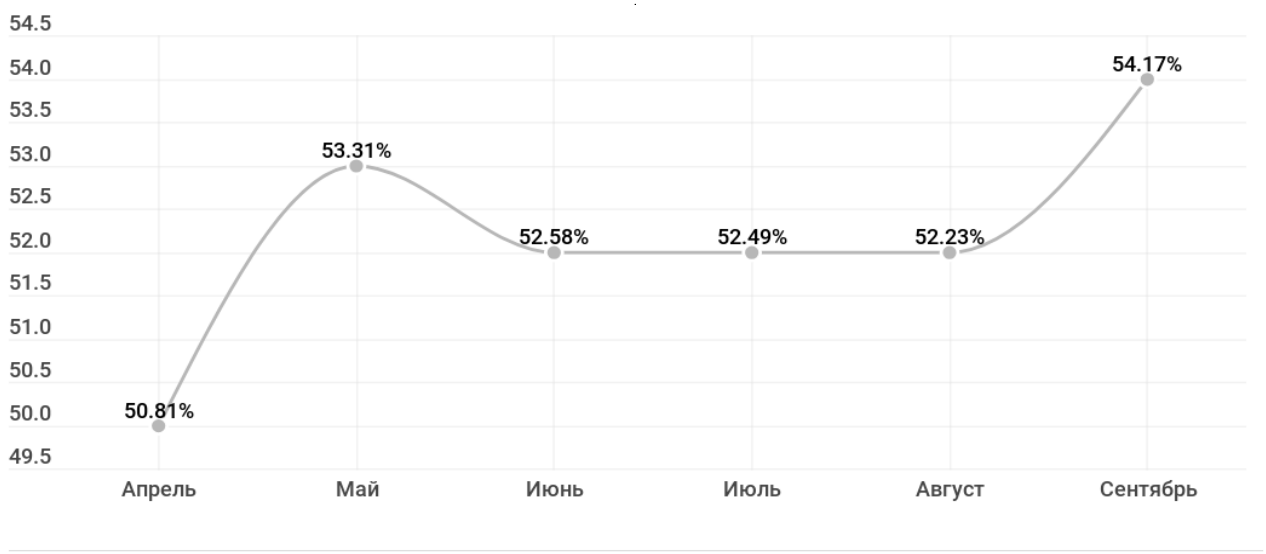

Рис. 10. Доля спама в почтовом трафике в русском интернете.

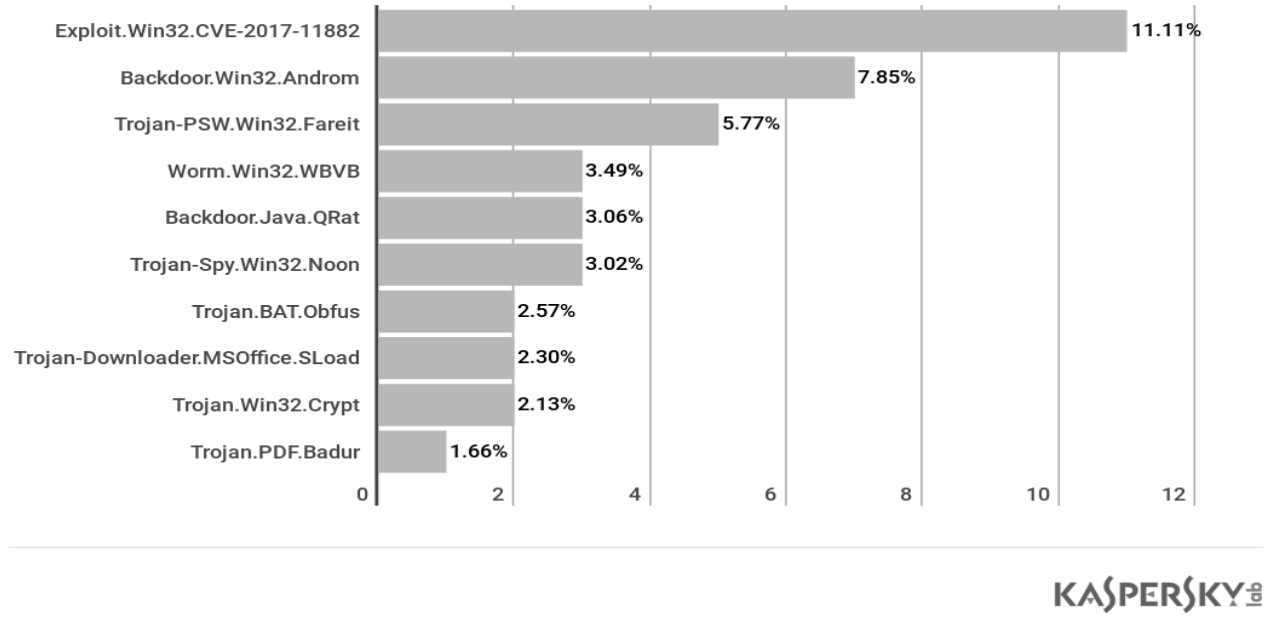

Рис. 11. Самые популярные вредоносные вложения за третий квартал 2018 год.

Данное вредоносносное программное обеспечение имеет функционал записи нажатия клавиш и последующий отправки их на сервер злоумышленника (рис. 9), и скачивания других вредоносных файлов по ссылкам (рис. 8), которые содержатся в теле, по команде злоумышленника.

Через подобный метод распространения на компьютер пользователя могут попасть любые другие вредоносные файлы. Например, Trojan-Ransom (Шифровальщики), они модифицируют данные на компьютере- жертве или блокируют работу компьютера, с целью дальнейшего выкупа за их расшифровку. Каждая программа этого поведения является инструментом для получения денежных средств киберпреступниками от ничего не подозревающих добропорядочных пользователей. Такие трояны используют множество различных алгоритмов

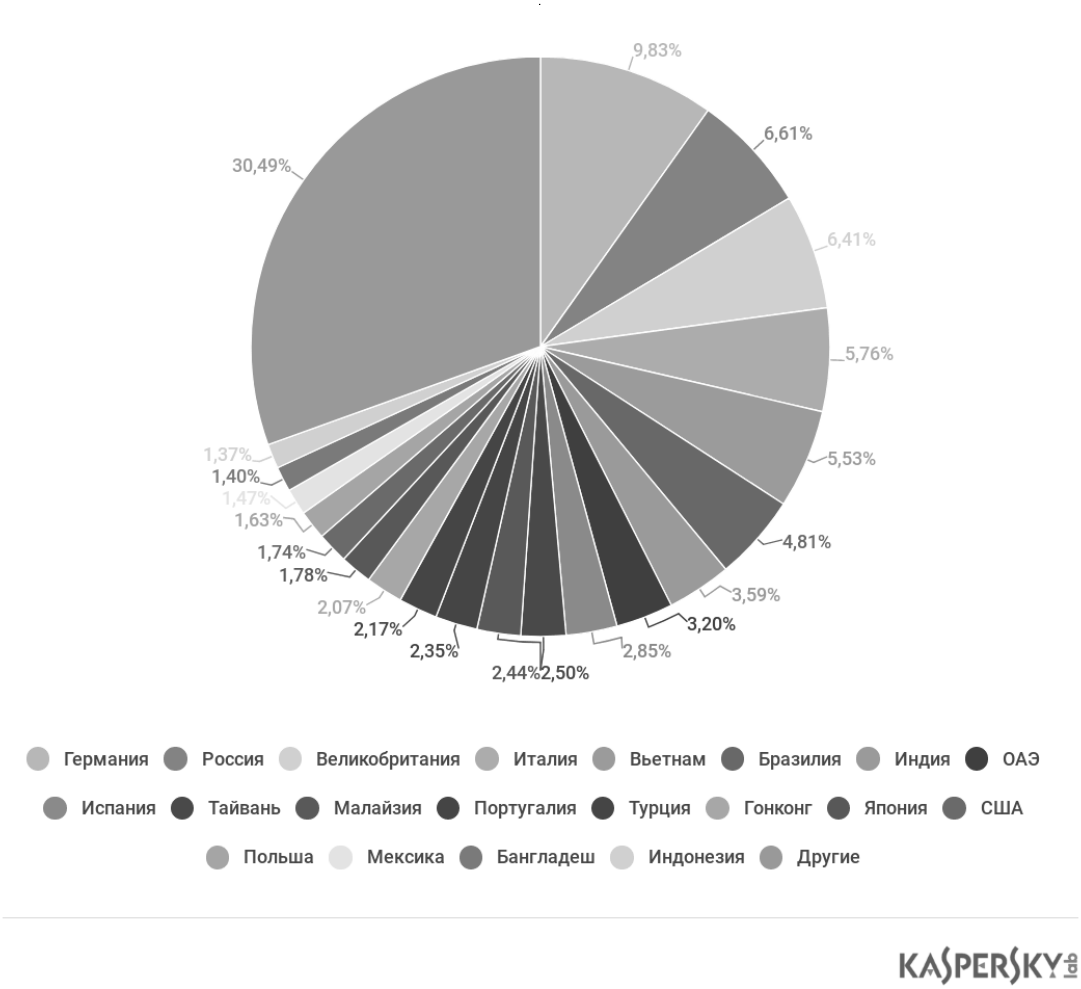

Рис. 12. Страны фишинговых атак.

шифрования пользовательских файлов, чтобы подобрать ключи для расшифровки файлов, зашифрованных трояном методом простого перебора, может потребоваться большое количество лет.

Статистика Спама и Фишинга

Лаборатория Касперского привела статистику спама в российском интернете за третий квартал 2018 года (рис. 10). Средний процент спама в почтовом трафике составил 52,54%.

Наибольшая доля спама была зафиксирована в сентябре — 54,17%.

Также Лаборатория Касперского предоставила список самых популярных вредоносных вложений за третий квартал 2018 год (рис. 11.).

Самым распространенным семейством стало **Exploit.Win32.CVE-2017–11882** — вредоносные объекты, эксплуатирующие уязвимость **CVE-2017–11882** в продукте Microsoft Word, которая позволяет выполнить произвольный код без взаимодействия с пользователем. [6]

Статистика фишинга в третьем квартале 2018 года оставляет желать лучшего: всего было предотвращено 137~<382~<124 попыток перехода пользователя на мошеннические страницы. Наибольшая доля атакованных пользователей было в Бразилии. Их доля составила 15,51%. [6] На рисунке 12 приведены страны фишинговых атак.

На первом месте Германия (9,83%), на втором — Россия (6,61%), а на третьем — Великобритания (6,41%). Четвертое и пятое места занимают Италия и Вьетнам (5,76% и 5,53% соответственно).

Рейтинг категорий организаций, атакованных фишинговыми атаками в третьем квартале 2018 года составила категория “Глобальные интернет-порталы”. Ее доля составила 32,27%. На рисунке 13 приведены категории

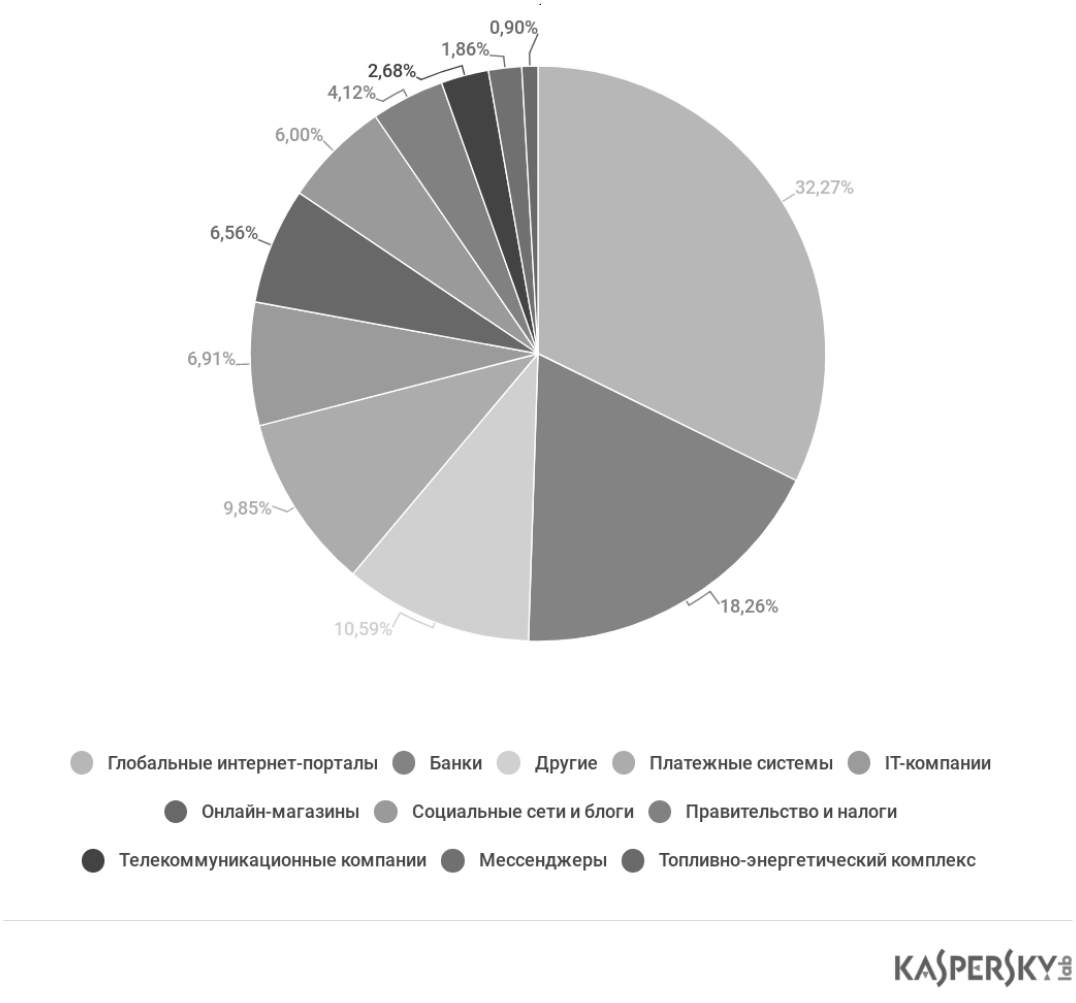

Рис. 13. Категории организаций, чьи пользователи были атакованы фишинговыми атаками.

организаций, чьи пользователи были атакованы фишинговыми атаками.

В основном, в этом квартале мошенники продолжают использовать громкие инфоповоды в своих схемах, к примеру, был «обыгран» выход нового iPhone. Кроме этого, ими продолжаются поиски каналов распространения мошеннического контента, и наряду с наращиванием активности в Instagram лабораторией Касперского были замечены поддельные уведомления от сайтов и вбросы фальшивых новостей с помощью медиаресурсов. Также стоит упамянуть рост спама с вымогательством, использующий реальные персональные данные жертв.

Рекомендации по защите от подобных атак

Итак, чтобы не стать жертвой злоумышленника, рекомендуется:

- Не открывать вложенный файл и не переходить по ссылкам в письмах, присланных незнакомыми людьми.
- Финансовые организации никогда не присылают писем с просьбой отправить им свои личные данные в электронном сообщении; перейти на сайт для авторизации или ввести личные данные во всплывающих окнах.
- Держать операционную систему и антивирусное ПО в обновленном состоянии.
- Использовать на компьютере антивирусную программу с защитой от спама и фишинга.
- Использовать при передаче конфиденциальных данных шифрованное соединение. Адрес защищенного соединения на сайте должен начинаться с http**s**, а в адресной строке или строке браузера должна быть иконка зеленого закрытого замочка.
- Не использовать магазины, зарегистрированные на бесплатных хостингах.
- Делать регулярное резервное копирование важных файлов.

ЛИТЕРАТУРА

1. Спам и фишинг https://encyclopedia.kaspersky.ru/knowledge/spam-and-phishing/ (Дата обращения 25.09.2018)
2. Michael S. Collins Network Security Through Data Analysis: Building Situational Awareness., 2014. 222 p. URL: http://index-of.es/Varios/Michael%20Collins-Network%20Security%20Through%20Data%20Analysis_%20Building%20Situational%20Awareness-O'Reilly%20Media%20(2014).pdf (Дата обращения 25.09.2018)
3. Victor Marak Windows Malware Analysis Essentials., 2015, 238p. URL: http://Ijo.es/Windows%20Malware%20Analysis%20Essentials.pdf (Дата обращения 25.09.2018)
4. Классификация вредоносных программ https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/ (Дата обращения 25.09.2018)
5. Сикорский М., Хониг Э., Вскрытие покажет! Практический анализ вредоносного ПО: Пер. с англ. под ред Питер 2018, 262 с.
6. Спам и фишинг в третьем квартале 2018 года https://securelist.ru/spam-and-phishing-in-q3–2018/92610/ (Дата обращения 09.11.2018)
7. Отчет по целевым кибератакам URL: https://securelist.ru/uvelichivaetsya-kolichestvo-apt-ograblenij-bankov-s-ispolzovaniem-atak-metel-gcman-i-carbanak-2–0/28044/ (Дата обращения 25.09.2018)

МИРЭА — Российский технологический университет